過剰な情報セキュリティ対策に関する組織論的な幾つかの視座

Some perspectives of excessive cyber-security in organization studies

間嶋　崇†
Takashi Majima†

† 専修大学 経営学部
† School of Business Administration, Senshu University

要旨:

近年，情報セキュリティの確保は，企業にとって重要な経営課題の一つである．それと同時に，日本では，業務遂行上の利便性とのバランスを欠いたセキュリティ対策の過剰なまでの厳格化やそういった現場からの認識が問題になっている．なぜなら，この過剰化は，生産性や革新性の妨げや現場の抜け穴探しなどの新たなリスクに繋がる可能性があるからである．本稿では、このような情報セキュリティ対策の過剰化がなぜ起きるのか，いかにしたら防げるのかについて議論するのに有用であろう 3 つ組織論的視座について検討していく．

Abstract:

Recently, cyber-security management is one of the most urgent management issues in Japan as well as other countries. And also, excessive cyber-security measures are highly controversial in Japanese companies. Because taking cyber-security measures too much bring them a deterioration in corporate productivity and increased new cyber-risks. Why do excessive cyber-security measures arise in many Japanese companies? How can their companies avoid lapsing into such strange measures? To answer these questions, in this paper we conduct a literature survey and discuss three perspectives in organization studies: practice, adaptive challenge, narrative mediation.

1.　はじめに

近年，サイバー攻撃などのサイバーリスクから身を守り，情報の安全性すなわち情報セキュリティを確保していくことは，日本企業にとって重要な経営課題の一つである[1]．一方で，セキュリティ対策が屋上屋を架すがごとく複雑で過剰になってしまったり，日々の業務上の不都合の生起よって営業や開発などの現場から過剰と認識されたりしてしまうこともしばしばである．同時に，それは，不都合を回避するためのシャドウ IT[2]などの抜け穴探しを惹起し，それによってさらにセキュリティが強化されるといった鼬ごっこを生んでいる．このような情報セキュリティの過剰対策がなぜ生まれ，どうしたら防げるのか．この問題は，新たなリスクを生むという意味でも現場の生産性や革新性を妨げるという意味でも回避すべき重大な課題である．且つこの問題は，技術的な問題であるのみならず組織的な問題であると考えられる．しかし，この問題を扱う組織論的な議論は，少なくとも日本国内においては皆無に等しい．そこで，本稿では，過剰な情報セキュリティ対策がなぜ生じ，それを防ぐにはどうしたらいいのかに関する幾つかの組織論的な視座を吟味していく．

まず次章では，問題背景として，企業を取り巻く情報セキュリティ問題の現状を明らかにしていこう．

2.　問題背景

2.1.情報セキュリティの重要性と現状

上述の通り，現在，企業にとって情報セキュリティは，喫緊の経営課題の 1 つである．コンピュータにまつわる情報セキュリティの重要性は, 2000 年代に入る以前から理解されていた［2］．しかし，その重要性の認識がさらに高まっていくのは，2000 年以降，すなわち，インターネットが商用化・普

表 1. 組織に対する情報セキュリティ上の脅威

順位	「組織」向け脅威
1	標的型攻撃による被害
2	ビジネスメール詐欺による被害
3	ランサムウェアによる被害
4	サプライチェーンの弱点を悪用した攻撃の高まり
5	内部不正による情報漏洩
6	サービズ妨害攻撃によるサービスの停止
7	インターネットサービスからの個人情報の窃取
8	IoT 機器の脆弱性の顕在化
9	脆弱性対策情報の公開に伴う悪用増加
10	不注意による情報漏洩

出典：［1］を参考に筆者作成

[1] もちろん世界的な課題でもある．

[2] シャドウ IT（shadowing IT）とは，自身の PC やスマートフォンなどのデバイスやクラウドサービスを自社の許可なしに勝手に業務に利用することである．企業側は把握できておらず，またセキュリティが脆弱な可能性もあり，リスクが高まる危険性を孕んでいる．自社に認められず，把握も出来ていない点で BYOD（bring your own device）と異なる．

及し，サイバー攻撃などによる情報漏洩のリスクなどがさらに拡大してからのことである［2］．さらに近年は，企業や社会の IT 依存度が増し，加えてサイバー攻撃手法の多様化やグローバル化，はたまた IoT 関連機器への侵入によるそれらの破壊など，新たな脅威も生まれ，リスクがさらに拡大・深刻化し，ますますその重要性の認識が深まっている［3］［4］（近年の組織に対する脅威については，表 1 も参照のこと）．これら深刻化するリスクを示す数字は様々あるが，例えば，日本経済新聞の 2019 年 12 月 16 日朝刊によれば，サイバー攻撃を受けた際の費用は，アメリカでは 2018 年に 2737 万ドルと 2012 年の 3 倍，日本でも 2018 年に 1357 万ドルと 2012 年の 2.6 倍にまで増えている[3]．また，サイバー攻撃含め，情報セキュリティに関するリスクは，このような経済的負担だけでなく，信頼の低下やシステムの停止による継続的な事業活動の困難性など，企業経営に重大な損失をもたらす［5］。

日本における情報セキュリティへの関心あるいはそれに関わるリスクの高まりは，メディアや論文・雑誌記事の数からも窺い知ることができる．表 2 と図 1 は，日経テレコン，J-Stage（科学技術情報発信・流通総合システム），CiNii（国立情報学研究所学術情報ナビゲータ）における情報セキュリティないしサイバーセキュリティをキーワードとする新聞記事，それらをタイトルとする論文・雑誌記事の件数とその推移（1980 年から 2019 年までの 40 年間）である。情報セキュリティに関する記事や論文は，1984 年にすでに存在している。ちなみに，この新聞記事は，暗号技術に関するコラム記事（日経産業新聞 6 月 19 日）であり，論文は，すべて情報処理学会の学会誌『情報処理』の情報セキュリティ特集に寄せられた論稿である。コンピュータ犯罪やそれを防ぐための個人識別技術・暗号技術などがそれぞれの論考の主題になっている。しかし，研究にしても新聞記事にしても 90 年代後半から徐々に件数が増加し，本格的に注目され重要性が認識されるのは，やはり 2000 年以降であることが図表からわかるだろう．とりわけ 2010 年代は，非常に注目が高くなっている．もちろん，この増加には，スマホや電子決済の普及によって，個人がリスクに晒される機会が増えていることも手伝っているが，度々の記述の通り企業の晒されるリスクのますますの複雑化と深刻化の現れでもあるだろう[4]．

2.2.過剰な情報セキュリティ対策

このような状況の中，情報セキュリティを確保するために，企業においては様々な対策が施されることになる[5]．例えば，総務省によれば，表 3 のような取り組みが挙げられる．ただし，これらは，あくまで大枠の提示であり，実際，技術的にはさらに多様且つ複雑で，加えて新たな脅威に合わせてどん

表 2. 情報セキュリティへの関心

年	J-Stage	CiNii	日経テレコン
1980	0	0	0
1981	0	0	0
1982	0	0	0
1983	0	0	0
1984	0	13	1
1985	0	0	0
1986	0	0	2
1987	1	1	0
1988	1	6	3
1989	0	3	1
1990	0	2	1
1991	0	18	1
1992	0	1	3
1993	1	2	1
1994	1	13	3
1995	2	30	6
1996	1	33	9
1997	1	31	7
1998	1	43	5
1999	0	45	14
2000	0	106	36
2001	3	126	37
2002	5	157	50
2003	3	160	91
2004	3	193	173
2005	12	267	216
2006	8	233	177
2007	21	286	142
2008	6	192	103
2009	9	235	111
2010	24	177	78
2011	10	184	109
2012	10	218	113
2013	9	340	160
2014	8	295	185
2015	15	300	203
2016	9	428	207
2017	16	380	220
2018	8	329	247
2019	9	298	214
合計	197	5145	2929

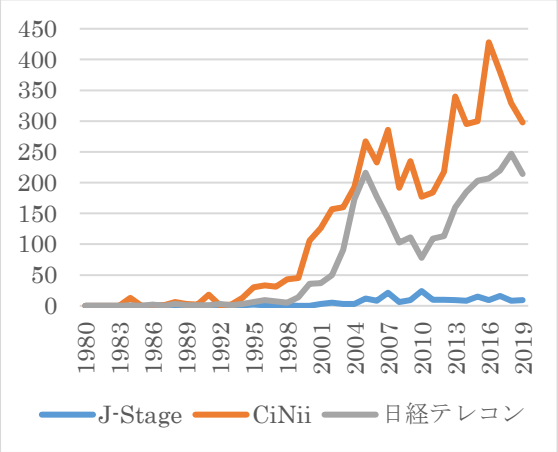
出典：筆者作成

[3] 他にも個人情報漏洩は，損害賠償として，一事案平均 5 億 4850 万円と推計されている［3］．また，委託企業の従業員に不正に顧客情報を持ち出されたある企業の株価は，事件の前後で会員顧客数が 30%減少，株価も 20%（約 720 億円）下落してしまった［5］．以前のサイバー攻撃は，ある意味優れたスキルを持った者のそのスキルの誇示を目的とした愉快犯であることが多かったようだが，2004 年頃から，金銭目的の犯罪，さらに近年はハッカー集団による組織的犯罪へと変化しているようである［6］．

[4] 個人への脅威の増加の現れとして，独立行政法人情報処理推進機構（IPA）の毎年発刊している「情報セキュリティ 10 大脅威」も 2016 年版から個人への脅威と企業など組織体への脅威とを分けて提示するようになってきている。

[5] 国としても 2005 年に内閣官房情報セキュリティセンター（現：内閣官房サイバーセキュリティセンター）の創設を契機に，2014 年にサイバーセキュリティ基本法を制定，2015 年にサイバーセキュリティ戦略を閣議決定するなど，国全体としての情報セキュリティの向上に努めている［3］．

図 1.情報セキュリティへの関心の高まり



出典：筆者作成

表 3. 情報セキュリティ対策の例

ウィルス感染	ウィルス対策ソフトの導入
	ソフトウェアの更新
	危険な web サイトのフィルタリング
不正侵入	パスワード管理
	ファイアウォールの導入
	侵入防止システムの導入
	ソフトウェアの更新
	ログの取得と管理
情報漏洩	ファイアウォールの導入
	顧客データなどの管理
	資料、メディア、機器の廃棄ルールの徹底
	無線 LAN のセキュリティ設定
	ユーザー権限の管理
	パスワード管理
災害などによる機器障害	バックアップ
	無停電電源装置の設置
	設備の安全管理

出典：[7] を参考に筆者作成

どん変化していく．各企業は，これらの取り組みを，その企業の状況に合わせて取捨選択，あるいはトリアージしながら，多層的に展開していくことが求められている［5］［8］．しかし，その一方で，日々の業務上さまざまな不便（業務効率や革新性の低下の恐れ）が生じ，営業や開発など情報セキリュティ以外の部署の従業員から過剰で面倒だと認識されてしまうほど，複雑且つ厳格あるいは盛り沢山のセキュリティ対策が展開されてしまうケースも実際あちこちで見受けられる[6] ［8］．例えば，各種パスワードの定期的な変更義務や指定外のアプリケーションやクラウドサービスの利用禁止，一部 Web サイトの閲覧制限，USB メモリの使用禁止などは，現場にとって面倒や不便を感じる対策のようである．このような手間や不便は，時に，シャドウ IT など，それを回避するための抜け穴探しを惹起する危険性を孕んでいる．それゆえ，この危険性は，情報セキュリティ部門によるさらなるセキュリティ強化を促す。それに対して，その他の部署は，新たな抜け穴を探し，それに対してセキュリティ部門は新たに…と果てなき鼬ごっこが生みだされていく．このような鼬ごっこによって情報セキュリティ対策は，ますます過剰化していく．本来，業務の利便性とのバランスが肝要であるが，なぜこのような情報セキュリティ対策の過剰化が進んでしまうのであろうか．どうしたら防げるのであろうか．

3. 問題意識と方法

前章の最後に示したように，本稿筆者の問題意識は，「情報セキュリティ対策の過剰化はなぜ生じ，それはどうしたら防げるのか？」である．この問題を指摘する文献やコラムはあるものの，それを主題にした研究は今のところ見当たらない．またこの問題は，セキュリティに関する技術的な問題でもあるが，それにとどまらず過剰に厳格化を進めてしまうような部門間の関係性や規則とその遵守・逸脱など，極めて組織的な問題でもある．そこで，本研究では，この問題を組織論の観点から吟味したいと考えている．しかし，そもそも，情報セキュリティの問題を組織論的観点から検討する先行研究が少ない．図 1 と表 2 で日本において先行する論文や記事の数を紹介したが，例えば，CiNii では，情報セキュリティないしサイバーセキュリティで検索すると，5145 件の論文ないし雑誌記事がヒットする．しかし，「情報セキュリティ，組織」，「サイバーセキュリティ，組織」と検索すると，わずか 104 件に絞られる[7]．さらに，その中身を見ていくと，実際に組織論的観点から議論しているものは，ごくわずか，10 件程度である［9］［10］［11］［12］［13］［14］［15］［16］［17］［18］．そして，そのいずれもが本研究の問題意識とは異なる問題意識を探究するものである[8]．そこで，本稿は，過剰な情報セキュリティ対策の発生のカラクリやその防止策を明らかにするという本研究の大きな目的の第一弾として，すなわち，定性ないし定量的な調査の前段として，本研究の問題意識の解明に有用と考えられる幾つかの組織論的な視座を先行する文献を通じ検討・提示していくことにしたい．

[6] 顧客に対する厳格すぎるセキュリティ要求，例えば複雑なパスワードでのアカウント管理の要求などは，面倒がられて顧客離れを生む可能性があるようだ［8］．

[7] 同様の検索を J-stage でしてみると，197 件中わずか 2 件である．もちろん，検索の仕方により漏れているものをあるだろう．また，Academy of management の各誌，Organization Science，Organization Studies, Organization を検索しても組織論的観点による情報セキュリティ研究はわずか 3 件程度であった（2020 年 1 月現在）

[8] 情報セキュリティの有効性をいかにしたら高められるかという点においては，そのどれもが本研究と共通の問題意識に立脚している．

4.　過剰な対策に対する組織論的な幾つかの視座

4.1.実践としての情報セキュリティ

まず，情報セキュリティを過剰に厳格化していく引き金であり，さらに強化，エスカレートさせてもいる従業員たちの「情報セキュリティ対策を遵守しない」「抜け穴を探す」という行為に関する 1 つの研究視座として，実践(practice)に関する研究を挙げることが出来よう．2000 年代に入り，経営学では，実践としての経営戦略（strategy as practice）や実践としての経営倫理（business ethics as practice）など，組織成員たちが「戦略」や「倫理」を使いながら，その下で実際にどのような行いをしているのかを明らかにする研究視座に注目が集まった［19］［20］．例えば，実践としての経営倫理研究では，経営倫理綱領や内部通報制度など，さまざまな組織を倫理的にするための施策がその施策の作り手の意図とは異なる用いられ方で異なる実践を生み出していること，そしてそれは時に施策の作り手の道徳観とは真逆の実践を生み出していることを明らかにした［21］［22］．もう少し具体的には，例えば，ある企業では倫理綱領が部下に対する権力行使やパワハラの道具として使われていたり，あるいは別の企業では対外的な正当性や評判の確保の道具として利用され従業員たちは自分たちには関係のないものと捉えていたりしたのである［23］［24］．このように，人は，施策に従って行為するのではなく，それらをある種のリソースとして使って行為するということである[9]．このことは，作り手からすれば，「作者の死」が起きているとも言えるかも知れない［25］．施策を形にした途端，その複雑な策定プロセスや作り手の思いの細部，施策の意味などがブラックボックスの中に閉じ込められ，伝わりにくくなり，そのことで施策の下で働く組織の構成員は自分たちの文脈の中でそれを意味づけ，そこでの実践に向け利用する（あるいは利用しない）のである．

情報セキュリティ対策も同様のことが言えるだろう．情報セキュリティ部門の策定したさまざまなセキュリティ施策は，策定され実施された途端にその背景（プロセスや意味など）がブラックボックス化し見えづらくなる．にもかかわらず遵守を迫られる．その中で，その他の部署は自分たちの文脈の中でそれらを意味づけし，作り手であるセキュリティ部門の想定とは異なる実践（シャドウ IT など）を生み出していくのである．

これらは，情報セキュリティ対策の過剰化を促す引き金のカラクリを示すに有効な視座の一つと考えられるだろう．また，この視座に立つならば，作者の死あるいはブラックボックス化をいかに防ぐか，また同時に現場の置かれた文脈を理解することが過剰化やそのループの引き金を引かないための重要なポイントであると言うことができるであろう．

4.2.適応課題としての情報セキュリティ対策の過剰化

前項から分かることは，情報セキュリティは，その技術的な対策を厳格にしていけば確保出来るわけではなさそうで，もっと複雑で，実際の確保には，部門間の立場の違いや置かれた状況から生じる互いの理解し難さのようなものを互いに乗り越える必要がありそうだということである．しかし，それを無視し，技術的な対策の厳格化をますます推し進めていくことで，情報セキュリティを確保しようとすることが，すなわち情報セキュリティ対策の過剰化問題であると理解することが出来る．技術的対策への邁進は，実際は相互理解の困難性をさらに深め，さらなる逸脱的実践を再生産するに過ぎないのである．これは，ハイフェッツとリンスキー（R.Heifetz and M.Linsky）の言う「適応課題(adaptive challenge)」を「技術的問題(technical problem)」として扱ってしまうことによって生じた事象と説明することが出来よう［27］［28］．

ハイフェッツらによれば，「技術的問題」とは，既存の専門知識や手順を用いて解決可能な問題のことを指す．一方で，「適応課題」は，複雑な組織環境の変化の中で生じ，技術的な解決策は役に立たず，自分を含めた人々の価値観や習慣，信念などの変更，それに伴う痛みを許容しなければ解決出来ない問題のことを指す［27］［28］.また，この問題は，問題の特定にも問題の解決にも学習を要し，自分を含めた人と人，組織と組織の間の関係性の中で生じる問題である［28］［29］．ちなみに，この適応課題には，表 4 にあるように 4 つの基本パターンがある［28］．

ハイフェッツらによれば，このような解決困難な適応課題にチャレンジするためには，何を変え，何を変えてはならないかを見極めながら，問題に対して観察・解釈・介入していくリーダーシップが必要である［28］．

情報セキュリティ対策の過剰化の問題は，技術的問題の側面ももちろんあるが，技術的対応だけでは解決し得ない人と

表 4. 適応課題の 4 つのパターン

類型	名称	概要
1	大切にしている 価値観と行動のギャップ	組織が推奨する価値と実際の取り組み（組織内の諸制度やマネジメント行動）との間の矛盾が生じるという問題.
2	コミットメントの対立	組織が達成すべきミッション間の対立の問題. 例えば部門間のミッションの対立など.
3	言いにくいことを 言わない	頭の中で思っていてもそれを口に出さない，出せないという問題。例えば，急進的な考え方，難しい課題の指摘，対立する見解の痛みを伴う判断が心の中に飲み込まれることで問題発見や解決の遅れが生じる.
4	回避行為	適応を要する変化や変革がもたらす痛み・苦痛から逃げようとする問題. 例えば，適応課題を技術的問題とし対応しようとする「問題のすり替え」や問題誰かのせいにしたり、誰かに押し付けたりする「責任転嫁」など.

出典：［29］を参考に筆者作成.

[9] 文脈は異なるが，明示的ルーティンと遂行的ルーティンの関係とも似ている［26］.

人，組織と組織の関係性から生じる適応課題であると言えよう．確固たることは，実際の調査を待たなければならないが，過剰化は，上述の基本的パターンのとりわけコミットメントの対立と回避行動（問題のすり替え）によって惹起される問題であると推測しうる．すなわち，万全なセキュリティをミッションとする情報セキュリティ部門と売上や利益といった業績にコミットする営業部門など他部門との間のコミットメントの対立が生じ，その中で他部門による抜け穴探しの実践が生まれ，またそれを情報セキュリティ部門は技術的な問題として対策の強化をもって解決しようとすることで起きている問題として理解できるのである[10]［30］．

以上のハイフェッツらの議論は，情報セキュリティの過剰化の背後にある本質的な問題を明らかにするのに有効な視座であると言えるだろう．また，この視座に立つならば，この問題が適応課題であることを認識し，とりわけコミットメントの対立をいかに解消していくかが過剰化解消のポイントになると言えるだろう．

4.3.ナラティヴの対立/対立のナラティヴの解消

では，この適応課題を乗り越えるには，いかにしたらいいだろうか．その手がかりを与えてくれそうな第 3 の視座が対話型組織開発，とりわけナラティヴメディエーションである[11]［31］．

まず対話型組織開発とは，社会構成主義をベースに，人々の語りと，その語りや行為あるいは理解の背後にあるナラティヴ（物語）やディスコース（言説）に目を向け，組織の変革（組織の健全性の確保）を目指す議論である［31］．

この対話型組織開発によれば，組織の変革による組織の健全性の確保は，対象者たちの対話を通じて，人々の寄って立つ核となるナラティヴそして現実の構成に変化を与え，そのことで新たな行為を導出する新しい見方・考え方（生成的なイメージ）を生み出すことによって可能になる［31］(表 5 も参照のこと)。

本稿に寄せて説明するならば，情報セキュリティ対策の過剰化の解消は，異なるミッションや状況下で異なるナラティヴつまり異なる現実を生きるさまざまな部門を集め，それぞれが対話することで，核となるナラティヴに変化を与え，情報セキュリティに対する新たな見方や行為を導出すること

表 5. 対話的組織開発における変革プロセス

プロセス 1	現在における現実の社会的構成に創造的破壊が生じ，より複雑な再組織化が行われる．
プロセス 2	1 つまたは複数の核となるナラティヴに変化が生じる．
プロセス 3	生成的イメージが導入されるか，または自然に表れ，思考と行動のための新しい説得力のある代替案を提供する．

出典：［31］を参考に筆者作成．

でなしうると考えられる．

さて，その変革のプロセスを牽引するにあたり，組織開発のファシリテーターたち（コンサルタントなど）が担う役割は，自らも現実の構成に影響を与えるシステムの一部であることを理解しながら，生成的なイメージが生まれるような機会を創ることである［31］. そのファシリテートの手法ないしアプローチには，AI（appreciative inquiry）やワールドカフェなど，ブッシュとマーシャク（G.Bushe and R.Marshak）によれば，少なくとも 40 の方法があるようだが，そのうちの一つが先述したナラティヴメディエーションである［31］.

ナラティヴメディエーションとは，組織の健全性確保，その中でも，人と人，組織と組織の対立の解消に焦点を当てたアプローチである[12]［32］．同アプローチは，従来の「利害対立」の解消に焦点を当てたメディエーション（調停・仲裁）とは異なり，各自の生きるナラティヴの相違やそこから眺める（構成した）現実から生じる「対立のナラティヴ」の解消に焦点を当てている．すなわち，調停者が対立する当事者たちとの対話を通じて，対立のないあるいはそれが和らいだ代替的なナラティヴの再著述を共同で行っていくのである．

同アプローチは，ナラティヴセラピー[13]の影響を強く受けており，同セラピーで用いられる手法がふんだんに用いられているのも特徴である．例えば，調停者は，自身のナラティヴを当事者たちに押し付けないように「無知の姿勢」で当事者たちの語りに耳を傾ける［32］［33］．加えて，当事者たちが支配されている対立のナラティヴ（それを組み立てている思い込み）を脱構築するために，「問題の外在化」，「問題の名付け」，「問題の歴史化」を行っていく［32］［34］［35］．さらには，「ユニークな結果」を用いて，支配的だった対立的なナラティヴに代わるナラティヴを共同で見出し構築していくのである［32］［35］（表 6 も参照のこと）．

表 6. ナラティヴメディエーションの技法

問題の外在化	当事者ではなく問題に注目するために，問題を当事者たちから切り離し，当事者たちに内在する問題ではなく，外側に在るものと捉える技法．
問題の名付け	外在化のための方法．問題を客体化するために問題に名前をつける．
問題の歴史化	問題の外在化をさらに進める方法．名前の付けられた問題の誕生から現在までのその変化や展開をある種の物語として時間軸の中に位置付ける．
ユニークな結果	代替的なナラティヴを構築するためのきっかけを見出す材料．支配的なナラティヴに合致しない（ユニークである）が故に，まだ語られていない体験のこと．

出典：［32］を参考に筆者作成

[10] ここでは営業部門を例にとったが，経営陣や顧客，株主などさまざまなアクター間のコミットメントの対立が推測出来る．

[11] ［31］ではハイフェッツらの議論が引き合いに出され，適応課題を克服するには対話型組織開発が有用であることが示されている．なお，対話型組織開発は，ポストモダン的転回を標榜しており，ナラティヴアプローチに限らず，複雑系科学なども取り入れて展開しているが，本稿では，ナラティヴアプローチに焦点を当てて議論していく．

[12] ただし，このナラティヴメディエーションの捉え方は，狭義であろう．同アプローチは，組織の開発のみならず，広く様々な対立構造の解消を目指した議論である［32］．

[13] 精神医療で用いられるナラティヴアプローチのことである［33］

本稿の問題意識である情報セキュリティ対策の過剰化の問題も，根本的には，異なるナラティヴと現実を生きる部門間の理解困難性から生じる対立のナラティヴの問題であると捉えることができる。さらにこの視座に従えば，問題の外在化など，上記の対話の手法を用いながら支配的なナラティヴ（対立のナラティヴ）を脱構築し，代替的なナラティヴへと書き換えることで問題の解消が可能になると考えられる．

5.　結びにかえて

本稿では，情報セキュリティ対策の過剰化問題を取り上げ，この問題を吟味する上で有用であろう 3 つの組織論的視座について検討してきた．すなわち，実践，適応課題，ナラティヴメディエーションの 3 つである．それぞれは，過剰化の引き金となる逸脱行為の発生図式，過剰化を生じさせる背景にある組織的問題，過剰化の背景の組織的問題を解消する方法と，同問題の異なる側面を照射する視座であった．本稿は，これまであまり研究されてこなかった問題の重要性を指摘し，さらにそれらを理論的に検討することで，研究としての一定の貢献を果たしたと考えられる。しかし，当然のことながら，これら提示した視座の研究上ならびに実践上の有用性は，今後の調査研究を待たねば確かなことは分かりえない．本稿の成果は，問題の端緒を開いたばかり，本研究の序説の序説に過ぎないと言えるだろう．

さらに，本稿で取り上げた理論的視座以外にも，本研究対象の分析の切り口として考えられる視座はまだまだあるだろう．例えば，制度派組織論や新制度派社会学の組織分析などである．これらの視座は，本稿であまり触れられてこなかった過剰化を巡る組織の外のアクターとの関係性を見ることが出来そうだ．それゆえ，本稿は序論としても課題が山積し，さらなる検討が必要である．

謝辞

本稿は，「平成 29 年度相馬学術奨励基金海外研究員」の研究成果であり，本研究員期間に着想を得た筆者の研究テーマ「テクノロジーを媒介にした組織の倫理の生成」の一部である．支援に対し，記して感謝したい．

参考文献

[1] 独立行政法人情報処理推進機構セキュリティセンター，情報セキュリティ 10 大脅威 2019 年版，独立行政法人情報処理推進機構，2019.
[2] サイバーセキュリティと経営戦略研究会，サイバーセキュリティ，NTT 出版，2014.
[3] 谷脇康彦，サイバーセキュリティ，岩波新書，2018.
[4] 日本経済新聞社編，まるわかり！サイバーセキュリティ，日本経済新聞社，2019.
[5] 横浜信一，経営とサイバーセキュリティ：デジタルレジリエンシー，日経 BP 社，2018.
[6] 独立行政法人情報処理推進機構セキュリティセンター，情報セキュリティ 10 大脅威 2016 年版，独立行政法人情報処理推進機構，2016.
[7] 総務省，安心してインターネットを使うために：国民のための情報セキュリティサイト（https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html）
[8] 島田裕次，この 1 冊ですべてわかる情報セキュリティの基本，日本実業出版社，2017.
[9] 中西晶，”情報セキュリティにおける高信頼性組織概念の適用”， 2006 年春季経営情報学会全国研究発表大会要旨集，pp.47-47,2006.
[10] 寺本直哉，”実践共同体としての遊び:情報セキュリティ組織の人材育成を事例として”，經營學論集 80，pp.F21-1-F21-2, 2017.
[11] 寺本直哉ほか,”我が国における CSIRT の現状と課題”,2015 年秋季経営情報学会全国研究発表大会要旨集, pp.57-60,2015.
[12] 杉原大輔，”日本における企業内 CSIRT の現状と課題：NCA への早期加盟チームの実態から”，開智国際大学紀要 vol.17，pp.5-22,201.
[13] 北野晴人，“組織コミットメントからみた内部不正行為の抑止に関する考察”， 経営行動科学学会年次大会：発表論文集 (17), pp.391-396, 2014.
[14] 吉田健一郎，島田達巳，“情報セキュリティ意識の普及--ジョンソン・アンド・ジョンソンの事例を中心として”，日本社会情報学会学会誌 21(2), pp.35-45, 2010.
[15] 伊藤俊之，廣松毅，”情報セキュリティにおけるリスクコミュニケーション”，2010 年秋季経営情報学会　全国研究発表大会要旨集, pp.20-20, 2010.
[16] 浜屋敏，”情報セキュリティ対策の望ましいガバナンス構造”， 2009 年秋季経営情報学会全国研究発表大会要旨集，pp. 80-80, 2009.
[17] 吉田健一郎，”組織倫理・情報セキュリティ・情報倫理の構図”，麗沢大学紀要 vol.86, pp.169-182, 2008.
[18] 樋口晴彦，” ベネッセ顧客情報漏えい事件の事例研究”，千葉商大論叢 53(1), pp.155-171, 2015.
[19] Johnson. G., A. Langley, L. Melin, & R. Whittington, *Strategy as Practice: Research Directions and Resources,* Cambridge University Press,2007(高橋正泰監訳，宇田川元一，高井俊次，間嶋崇，歌代豊訳, 実践としての戦略：新たなパースペクティブの展開，文眞堂,2012.)
[20] Carter. C., S. Clegg, M. Kornberger, S. Lake, and M. Messner, *Business Ethics as Practice: Representation, Reflexivity and Performance*. Cheltenham,UK:Edward Elgar Publishing,2007.
[21] Gordon,R., S.Clegg and K.Kornberger, “Embedded Ethics: Discourse and Power in the New South Wales Police Service”, *Organization Studies* 30(1), pp.73-99,2009.
[22] Helin, S. and J. Sandström, “An Inquiry into the Study of Corporate Codes of Ethics”, *Journal of Business Ethics,* 75,pp.253-271,2007.
[23] Helin. S. and J. Sandström,“Resisting a corporate code of ethics and the reinforcement of management control”, *Organization Studies* 31(5),pp.583-604,2010.
[24] Helin. S. T. Jansen., J. Sandström and S. Clegg, “On the dark side of codes: Domination not enlightenment”, *Scandinavian Management Journal*.27,pp.24-33,2011.
[25] Barthes,R,Introduction à l'analyse strucuturale des récites. *Communications,* 8, pp.1-27,1966（花輪光訳,物語の構造分析，みすず書房,1979）
[26] Feldman,M. and B.Pentland., “Reconceptualizing Organizational Routines as a Source of Flexibility and

Change”, *Administrative Science Quarterly.*48,pp.94-118, 2003.

[27] Heifetz,R. and M.Linsky, *Leadership on the line:Staying alive through the dangers of change*, Harvard Business Review Press,2009（野津智子訳，［新訳］最前線のリーダーシップ：何が生死を分けるのか，英治出版,2018）

[28] Heifetz,R., M.Linsky, and A.Grashow,*The Practice of adaptive leadership*,Harvard Business Review Press,2009（水上雅人訳，最難関のリーダーシップ：変革をやり遂げる意志とスキル，英治出版,2017）

[29] 宇田川元一，他者と働く：「わかりあえなさ」から始める組織論，NewsPicks パブリッシング，2019.

[30] Majima,T., M.Udagawa, and M.Kurosawa,”Clinging to robustness:A paradoxical generation process of hyper-rigid cyber security system”,*SCOS/ACSCOS 2018 Tokyo: book of abstracts,* pp.84-85,2018.

[31] Bushe,G. and R.Marshak, *Dialogic organization development: The theory and practice of transformational change*, Berrett-Koehler Publishers, 2015（中村和彦訳，対話型組織開発：その理論的系譜と実践，英治出版，2018）

[32] Winslade,J. and G.Monk, Narrative Mediation: a new approach to conflict resolution, John Wiley & Sons, Inc.,2000.（国重浩一，バーナード紫訳，ナラティヴ・メディエーション：調停・仲裁・対立解決への新しいアプローチ，北大路書房，2010）.

[33] McNamee, S and K. J. Gergen, *Therapy as Social Construction*, London : Sage Publication,1992.(野口裕二，野村直樹訳，ナラティヴ・セラピー:社会構成主義の実践，金剛出版，1997)

[34] White,M and D.Epston,*Narrrative means to therapeutic ends*, Dulwich Centre Publications, 1990.（小森康永訳，物語としての家族，金剛出版，1992）

[35] White,M, Narrative therapy classics, Dulwich Centre Publications, 2017.（小森康永訳，ナラティヴ・セラピー・クラシックス：脱構築とセラピー，金剛出版，2018）